PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-207777
(43)Date of publication of application : 07.08.1998

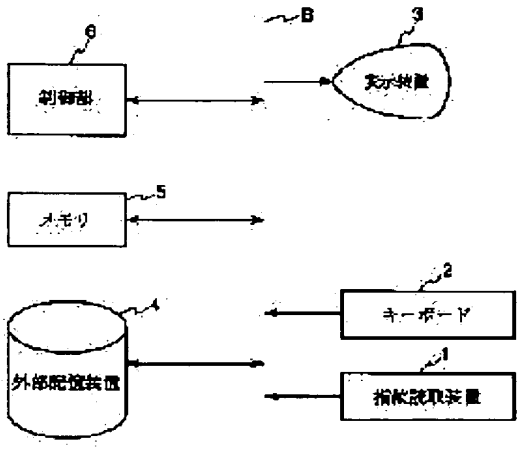
(51)Int.Cl. G06F 12/14
G06F 12/00
H04L 9/32

(21)Application number : 09-008065
(22)Date of filing : 20.01.1997

(71)Applicant : TSUBASA SYST KK
(72)Inventor : TSURUMURA YUKIZOU

(54) COMPUTER SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a computer system in which security can be improved without forcing the load of attention to a user.
SOLUTION: An encipherment algorithm is decided for each operator, and a file for storing a file to which access is permitted to each operator is enciphered and stored in an outside storage device 4. At the time of activation, the picture of the fingerprint of the operator is read by a fingerprint reading device 1. A control part 6 specifies the operator from the picture of the fingerprint of the user, and allows corresponding encipherment and decipherment programs to be resident in a main memory. Afterwards, it is possible to perform access to the file which can be deciphered by the resident decipherment program. The files of others are enciphered by different encipherment algorithms so that access can be inhibited.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平10－207777

(43)公開日　平成10年(1998)８月７日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	12/14	３２０	Ｇ０６Ｆ	12/14	３２０Ｂ
	12/00	５３７		12/00	５３７Ｈ
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７３Ｄ

審査請求　未請求　請求項の数５　ＯＬ　（全９頁）

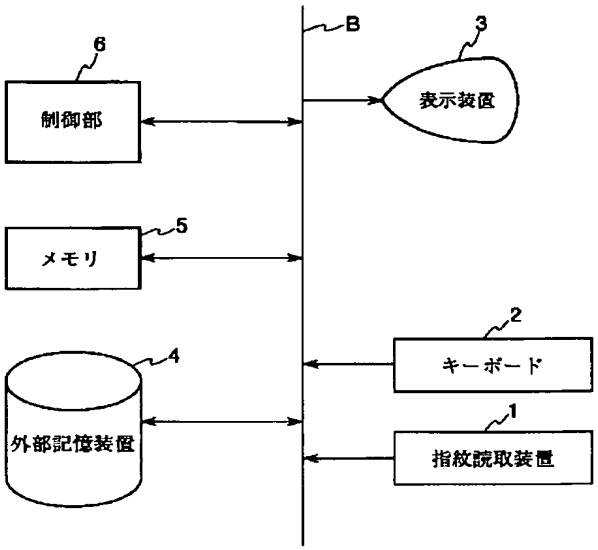
(21)出願番号　特願平9－8065

(22)出願日　平成９年(1997)１月20日

(71)出願人　594057314
翼システム株式会社
東京都江東区亀戸２丁目25番14号
(72)発明者　鶴村　亨三
東京都江東区亀戸２丁目25番地14号　翼システム株式会社内
(74)代理人　弁理士　木村　満　（外３名）

(54)【発明の名称】　コンピュータシステム

(57)【要約】
【課題】　ユーザに注意負担を強いることなく、セキュリティを高めることができるコンピュータシステムを提供する。
【解決手段】　外部記憶装置４に、操作者毎に暗号化アルゴリズムを定め、各操作者にアクセスが認められているファイルを格納するファイルを暗号化して格納する。起動時に、指紋読取装置１によって、操作者の指紋の画像が読み取られる。制御部６は、ユーザの指紋の画像から、操作者を特定し、対応する暗号化及び復号化プログラムを主メモリに常駐させる。以後、常駐している復号化プログラムで復号化できるファイルをアクセスできる。他者のファイルは、異なる暗号化アルゴリズムで暗号化されているため、アクセスすることはできない。



1

【特許請求の範囲】
【請求項１】複数の暗号化アルゴリズムを用いて暗号化された複数のファイルを記憶するファイル記憶手段と、操作者の身体情報と復号化アルゴリズムを対応付けて記憶する特徴記憶手段と、
外部より入力された操作者の身体情報に基づいて、前記特徴記憶手段を検索し、復号化アルゴリズムを特定する復号化アルゴリズム特定手段と、
前記復号化アルゴリズム特定手段により特定された復号化アルゴリズムにより前記ファイル記憶手段に記憶されたファイルを復号してアクセスする処理手段と、
を備え、
身体情報により特定された復号化アルゴリズムにより復号可能なファイルのみをアクセス可能としたことを特徴とするコンピュータシステム。
【請求項２】複数の暗号化アルゴリズムを用いて暗号化された複数のファイルを記憶するファイル記憶手段と、
前記ファイル記憶手段に記憶されたファイルと該ファイルのアクセスが認められている操作者の身体情報とを対応付けて記憶するアクセス許可条件記憶手段と、
前記ファイル記憶手段に記憶されたファイルへのアクセスの要求を検出する検出手段と、
前記検出手段が前記要求を検出した際に、操作者の身体情報の入力を要求する手段と、
外部より入力された身体的情報に基づいて前記ファイル記憶手段に記憶されたファイルへのアクセスが認められているか否かを前記アクセス許可条件記憶手段を参照して判別するアクセス許可判別手段と、
前記アクセス許可判別手段がアクセスが許可されていると判別した際に、該ファイルを復号するアルゴリズムを実行するためのプログラムをロードし、該プログラムを実行することにより前記ファイルをアクセス可能とするアクセス手段と、
を備えることを特徴とするコンピュータシステム。
【請求項３】前記暗号化アルゴリズムは、データを暗号化すると共に圧縮するアルゴリズムであり、前記復号化アルゴリズムは、暗号化されたデータを復号化すると共に伸張するアルゴリズムからなる、
ことを特徴とする請求項１又は２に記載のコンピュータシステム。
【請求項４】前記操作者の身体情報を読み取る身体情報読取手段と前記身体情報読取手段による身体情報の入力を促すメッセージを表示する手段を含む、
ことを特徴とする請求項１、２又は３に記載のコンピュータシステム。
【請求項５】前記身体情報は、指紋データ、網膜パターンのデータ、音声パターンのデータ、顔画像のデータのいずれかから構成され、
前記身体情報読取手段は、指紋読取装置、網膜パターン読取装置、音声パターン読取装置、顔画像読取装置のいずれかから構成される、

2

ことを特徴とする請求項４に記載のコンピュータシステム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、コンピュータのセキュリティ技術に関し、特に、指紋等の身体情報から各処理を実行する権限を有するか否かを判別するコンピュータシステムに関する。
【０００２】
【従来の技術】コンピュータの機密保護のため、ユーザ（操作者）名及びパスワードをコンピュータに予め登録し、ログオン時等にユーザ名及びパスワードを入力させ、入力されたユーザ名及びパスワードがコンピュータシステムに登録されていない場合、ログオンを認めない方法が知られている。
【０００３】
【発明が解決しようとする課題】しかし、ユーザ名及びパスワード等による機密保護では、他人が容易に推定出来ないようにパスワードを設定したり、パスワードを定期的に変更する等、ユーザに負担がかかる。また、システム管理者によりユーザＩＤ等が設定される場合には、ユーザＩＤを記憶、メモする等の負担がかかった。さらに、コンピュータシステムから要求がある度に、キーボード等からユーザ名、パスワード、ユーザＩＤ等を入力しなければならず、操作が煩雑であった。
【０００４】また、セッション中の各所で、実行を許可するか否かをユーザＩＤによってチェックする方法では、与えられたユーザＩＤやパスワードをメモしたり、記憶する等の必要があり、セッション中にユーザが離席して他者が着席する可能性があるため、機密保護の万全を期し難かった。
【０００５】この発明は上記実状に鑑みてなされたもので、ユーザに機密保護の負担をかけないコンピュータシステムを提供することを目的とする。
【０００６】
【課題を解決するための手段】上記目的を達成するため、第１の発明に係るコンピュータシステムは、複数の暗号化アルゴリズムを用いて暗号化された複数のファイルを記憶するファイル記憶手段と、操作者の身体情報と復号化アルゴリズムを対応付けて記憶する特徴記憶手段と、外部より入力された操作者の身体情報に基づいて、前記特徴記憶手段を検索し、復号化アルゴリズムを特定する復号化アルゴリズム特定手段と、前記復号化アルゴリズム特定手段により特定された復号化アルゴリズムにより前記ファイル記憶手段に記憶されたファイルを復号してアクセスする処理手段と、を備え、身体情報により特定された復号化アルゴリズムにより復号可能なファイルのみをアクセス可能としたことを特徴とする。
【０００７】上記目的を達成するため、第２の発明に係

るコンピュータシステムは、複数の暗号化アルゴリズムを用いて暗号化された複数のファイルを記憶するファイル記憶手段と、前記ファイル記憶手段に記憶されたファイルと該ファイルのアクセスが認められている操作者の身体情報とを対応付けて記憶するアクセス許可条件記憶手段と、前記ファイル記憶手段に記憶されたファイルへのアクセスの要求を検出する検出手段と、前記検出手段が前記要求を検出した際に、操作者の身体情報の入力を要求する手段と、外部より入力された身体的情報に基づいて前記ファイル記憶手段に記憶されたファイルへのアクセスが認められているか否かを前記アクセス許可条件記憶手段を参照して判別するアクセス許可判別手段と、前記アクセス許可判別手段がアクセスが許可されていると判別した際に、該ファイルを復号するアルゴリズムを実行するためのプログラムをロードし、該プログラムを実行することにより前記ファイルをアクセス可能とするアクセス手段と、を備えることを特徴とする。

【０００８】これらの構成によれば、操作者の身体情報に基づいて復号化アルゴリズムが特定される。従って、各操作者は、この復号化アルゴリズムを用いて復号できるファイルのみをアクセスでき、他のファイルをアクセスすることはできない。従って、正当権限を有する者のみが各ファイルをアクセスできる。また、ユーザ名、パスワード等をいちいち入力する必要がなく、操作性も高い。

【０００９】前記暗号化アルゴリズムは、データを暗号化すると共に圧縮するアルゴリズムであり、前記復号化アルゴリズムは、暗号化されたデータを復号化すると共に伸張するアルゴリズムからなる、ことが望ましい。このような構成とすれば、限られた容量のファイル記憶手段を有効に使用することができる。

【００１０】前記操作者の身体情報を読み取る身体情報読取手段と前記身体情報読取手段による身体情報の入力を促すメッセージを表示する手段を設けても良い。

【００１１】前記身体情報は、指紋データ、網膜パターンのデータ、音声パターンのデータ、顔画像のデータ等からなる。この場合、前記身体情報読取手段は、指紋読取装置、網膜パターン読取装置、音声パターン読取装置、顔画像読取装置等から構成される。

【００１２】

【発明の実施の形態】以下、この発明の実施の形態を図面を参照して説明する。

（第１の実施の形態）図１～図４を参照して、この発明の第１の実施の形態に係るコンピュータシステムを説明する。

【００１３】図１に示すように、このコンピュータシステムは、指紋読取装置１と、キーボード２と、表示装置３と、外部記憶装置４と、メモリ５と、制御部６と、これらを接続するバスＢから構成されている。

【００１４】指紋読取装置１は、人間の指紋の画像を読み取って、その画像データをＲＳ２３２Ｃインタフェース等を介してコンピュータ本体１に供給する。

【００１５】キーボード２は、文字、記号、数字等のデータを入力するための入力装置である。表示装置３は、ＣＲＴ、液晶ディスプレイ等から構成され、キーボード２から入力されたデータ、操作者へのメッセージ等を表示する。

【００１６】外部記憶装置４は、ハードディスク装置等から構成され、制御部６が処理するファイル（プログラム、文書ファイル、画像ファイル、等を含む）を暗号化された状態で記憶する。例えば、このコンピュータシステムをＡ，Ｂ，Ｃの３人で使用する場合には、図２に示すように、Ａのアクセスするファイルは暗号化アルゴリズムＨａで暗号化され、Ｂのアクセスするファイルは暗号化アルゴリズムＨｂで暗号化され、Ｃのアクセスするファイルは暗号化アルゴリズムＨｃで暗号化されている。外部記憶装置４は、制御プログラム１１とユーザマスタファイルを記憶する。ユーザマスタファイルは、Ａ，Ｂ，Ｃの指紋データと、暗号化プログラムＰＨａ～ＰＨｃと、復号化プログラムPHa^{-1}～PHc^{-1}を対応付けて記憶する。制御プログラム１１は、暗号化及び復号化プログラムを制御する。制御プログラム１１は、ＯＳ（オペレーティングシステム）の起動に続いて起動するように設定されている。

【００１７】メモリ５は、ＲＡＭ（Randam Access Memory）等で構成され、制御部６の主メモリ及びワークエリア等として機能する。制御部６は、ＭＰＵ（Micro Processing Unit）等で構成され、主メモリに格納されたプログラムを実行し、指紋読取装置１、表示装置３、外部記憶装置４に対して、それぞれ指紋読み取り、画像表示、データの書き込みもしくは読み込みを指示する。また、制御部６は、指紋読取装置１によって読み取られた指紋の画像データの処理、キーボード２から入力された文字等のデータの処理、表示装置３に表示する画面データの処理、外部記憶装置４からのデータの読み込み処理、外部記憶装置４へのデータの書き込み等処理を行う。

【００１８】次に、この実施の形態のコンピュータシステムの動作を図３のフローチャートを参照して説明する。このコンピュータシステムが起動されると、まず、ＯＳを起動し（Ｓ１１）、続いて、制御プログラム１１を起動する（Ｓ１２）。

【００１９】次に、制御プログラム１１は、指紋を入力すべき旨のメッセージを表示装置３に表示する（Ｓ１３）。さらに、指紋読取装置１に指紋の読み取りを指示する（Ｓ１４）。操作者はこの表示に従って指紋読取装置１から指紋を入力する（Ｓ１５）。指紋読取装置１は、読み取った画像データ（指紋の画像データ）をインタフェースを介してメモリ５に格納する。制御プログラム１１は、メモリ５に格納された指紋の画像データをコ

ード化し、コード化指紋データを生成する（Ｓ１６）。次に、コード化指紋データとユーザマスタファイルの指紋データを照合し（Ｓ１７）、一致するものがあるか否かを判別する（Ｓ１８）。

【００２０】一致するものがある場合には、その操作者がこのコンピュータシステムを使用することが認められていると判断し、図４に示すように、主メモリ（メモリ５）に制御プログラム１１と対応する暗号化・復号化プログラムを常駐させる（Ｓ１９）。以後は、データ読み出す時は、復号化プログラムを用いて暗号化されているプログラム・データ等を復号化して、読み出し、データ書き込む時は、暗号化プログラムを用いて暗号化してプログラム・データ等を書き込みながら、プログラムを実行する。

【００２１】一方、指紋読取装置１から読み取った指紋の画像データがユーザマスタファイルに登録されている指紋データのいずれとも一致しないと判断した場合（Ｓ１８）、制御プログラム１１は、その操作者がこのコンピュータシステムを使用することが認められていないと判断し、主メモリへの制御プログラム１１の常駐を中止する（Ｓ２０）。以後は、通常の動作に移行する。

【００２２】このような構成によれば、コンピュータの使用が認められている者の利用時は、制御プログラム１１と共に操作者に対応する暗号化・復号化プログラムが主メモリに常駐する。従って、図２に示すように、外部記憶装置４に格納されている各種データを復号化プログラムで復号して通常のプログラム又はデータとして読み出して、処理することができる。また、作成・加工したデータを、制御プログラム１１の制御下に暗号化プログラムを用いて暗号化して外部記憶装置４に格納することができる。

【００２３】しかも、コード化指紋データで特定される操作者に対応する暗号化・復号化プログラムのみが主メモリに常駐する。従って、各操作者は、他の操作者用の暗号化アルゴリズムで暗号化されたファイルをアクセスすることができない。従って、各ファイルへのアクセスを正当権限を有する者に限定することができる。一方、操作者が非登録者の場合には、制御プログラム１１が主メモリに常駐しない。従って、外部記憶装置４に格納されているプログラム及び各種データを復元することができない。従って、このシステム自体を使用すること自体が困難となる。

【００２４】例えば、操作者Ａがこのコンピュータシステムを使用する場合には、ＡはステップＳ１５で指紋を入力し、ステップＳ１６でこの指紋の画像データがコード化され、ステップＳ１８でＡの指紋の画像データから生成されたコード化指紋データとユーザマスタファイルのＡの指紋データが一致すると判別される。主メモリには、制御プログラム１１と共にＡ用の暗号化プログラムＰＨａとその復号化プログラムPHa^{-1}が常駐する（Ｓ１９）。

【００２５】従って、操作者Ａは、暗号化プログラムＰＨａを用いて暗号化されているプログラム１、２、文書ファイル１～３、画像ファイル等を復号化プログラムPHa^{-1}で復号化しながらアクセスし、さらに、作成及び加工した文書や画像を暗号化して外部記憶装置４に格納することができる。

【００２６】ここで、Ａが、例えば、Ｂがアクセス権を有するファイルをアクセスしようとしても、Ｂのファイルは暗号化プログラムＰＨｂにより暗号化されているので、主メモリに常駐している復号化プログラムPHa^{-1}では、これを復号化できない。従って、Ａは、Ｂのファイルをアクセスできない。従って、外部記憶装置４を共用しつつも、他者に秘密状態でファイルを使用できる。

【００２７】（第２の実施の形態）第１の実施の形態においては、ログイン時の個人認証に指紋データを使用したが、例えば、ファイルのアクセスが要求される度に操作者を認証することも可能である。このような処理を行う第２の実施の形態を以下に説明する。

【００２８】この実施の形態のコンピュータシステムの物理的構成は基本的に図１に示す構成と同一である。一方、この実施の形態のコンピュータシステムは、論理的には、図５に示すように、ＯＳ（オペレーティングシステム）２１と、ファイル制御プログラム３１とから構成されている。

【００２９】ＯＳ（オペレーティングシステム）２１は、キーボード２の入力操作を検出する入力部２２と、入力部２２により検出された入力指示に従った処理を実行する処理部２４と、表示装置３を制御する表示制御部２３を備える。処理部２４は、ファイルをアクセスするためのファイル処理部２５を含む。

【００３０】一方、ファイル制御プログラム３１は、イベントが発生したことを検出し、そのイベントがファイル操作に関するものである場合に、そのファイル操作を許可するか拒否するかを制御するためのプログラムである。

【００３１】図５は、ＯＳ２１が、ＤＯＳ（ディスクオペレーティングシステム）であるとした場合の例であり、ファイル制御プログラム３１は、入力フック部３２と、ドライバ部３３と、ユーザマスタファイル３９とから構成される。

【００３２】入力フック部３２は、割り込み要求が発行されたとき（イベントが発生したとき）、ファイル制御プログラム３１が存在しないときに行われるべき処理を行わせず、該処理に先立ちドライバ部３３に処理を行わせる（フックする）。

【００３３】ユーザマスタファイル３９は、図６に示すように、ユーザ毎、即ち、指紋データ毎に操作できるファイルのリストからなる。なお、このユーザマスタファイル３９自体は、このコンピュータシステムの管理者の

みがアクセスできるように設定されている。ドライバ部３３は、処理内容判別部３４と、メッセージ表示部３５と、コード化部３６と、判別部３７と、送信部３８とから構成される。

【００３４】処理内容判別部３４は、入力フック部３２により取り込まれた入力情報を解析し、その内容がファイルの操作を指示しているか否かを判別し、指示している場合には、コード化部３６に指紋の読み取りを指示すると共に判別部３７に入力情報を提供する。また、フックされた入力情報がファイルの操作を指示していない場合には、検出信号を送信部３８に送る。

【００３５】メッセージ表示部３５は、処理内容判別部３４が「入力がファイルの操作を指示している」と判別した場合に、指紋情報の入力を促す画面をＯＳ２１の表示制御部２３を介して表示装置３に表示する。また、判別部３７が「要求されたファイル操作がその操作者に認められていない」と判断した際に、アクセスが拒否されたことを示す画面を表示制御部２３を介して表示装置３に表示する。

【００３６】コード化部３６は、処理内容判別部３４からの指示に従って指紋読取装置１に指紋の読み取りを指示し、また、指紋読取装置１から指紋の画像を取り込み、これをコード化し、コード化指紋データを生成する。

【００３７】判別部３７は、コード化部３６で生成されたコード化指紋データに基づいて、ユーザマスタファイル３９を参照し、そのコード化指紋データを有する者が該当ファイルをアクセスする権限を有するか否かを判別する。そして、権限を有すると判断した場合には、送信部３８にアクセスを許可する信号を送信する。また、権限を有していないと判別した場合には、メッセージ表示部３５にアクセスを許可しない旨のメッセージを表示させる。

【００３８】第２の実施の形態のコンピュータシステムの動作を図７及び図８のフローチャートを参照して説明する。まず、コンピュータの電源が投入されると、ＯＳ２１が起動する（Ｓ３１）。次に、ファイル制御プログラム３１が起動する（Ｓ３２）。ファイル制御プログラム３１の入力フック部３２は、起動すると、ＯＳ２１の入力部２２が発生する割り込み要求に対応する処理のアドレスを、処理部２４からドライバ部３３のアドレスに書き換える。換言すると、入力部２２が発生するキー操作の検出信号等の送信先を入力フック部３２のアドレスに書き換える（Ｓ３３）。

【００３９】例えば、ＯＳ２１がマイクロソフト社から提供されているＭＳ－ＤＯＳ（登録商標）の場合には、主メモリとして機能するメモリ５上に作成される割り込みテーブル中、入力に関するシステムコールの割込ＩＮＴ２１に対応する処理のアドレスをドライバ部３３のアドレスとする。以上で、起動時の設定動作は終了する。

【００４０】この状態で、キーボード２から何らかの入力があると、ＯＳ２１の入力部２２は、この入力操作を判別し、必要に応じて割り込み要求を発する（ＩＯイベントの発生）。この割り込み要求に対応する処理は、通常は処理部２４で行うが、ファイル制御プログラム３１の起動時にドライバ部３３のアドレスに書き換えられている。従って、処理はドライバ部３３に移行され、フックされる（図８、Ｓ４１）。

【００４１】処理内容判別部３４は、ＯＳ２１から入力された検出信号を解析し（Ｓ４２）、入力内容がファイルの操作（ファイルを開く、実行ファイルを起動する等）を指示しているか否かを判別する（Ｓ４３）。入力内容がファイルの操作を指示している場合には、コード化部３６を介して指紋読取装置１に指紋の読み取りを指示する（Ｓ４４）。さらに、メッセージ表示部３５に指紋の入力を促すメッセージの表示を指示する（Ｓ４５）。メッセージ表示部３５は、処理内容判別部３４の指示に従い、ＯＳ２１の表示制御部２３を介して表示装置３に、指紋の入力を促すメッセージを表示する。

【００４２】コード化部３６は、指紋読取装置１からの指紋の画像データの入力を待機し（Ｓ４６）、画像データが入力されると、この画像データをコード化指紋データに変換し、判別部３７に提供する（Ｓ４７）。判別部３７は、ユーザマスタファイル３９を参照し、コード化部から供給されたコード化指紋データを有する者が、入力操作で指示されたファイルの操作を認められているか否かを判別する（Ｓ４８）。

【００４３】判別部３７は、アクセスが認められていると判断すると、主メモリにそのファイルをアクセスするために必要な暗号化プログラムと復号化プログラムを常駐させる（Ｓ４９）。続いて、判別部３７は、送信部３８に検出信号を供給する。送信部３８は処理をＯＳ２１の処理部２４に引き渡す（Ｓ５０）。

【００４４】以後、処理部２４は、復号化プログラムにより指示されたファイルを復号化して読み出し、加工・生成したデータを暗号化プログラムにより暗号化して書き込む。そのファイルのアクセスが完了すると、ファイル制御プログラム３１は、主メモリ上の圧縮プログラム及び復号化プログラムを削除する。

【００４５】一方、ステップＳ４８で、判別部３７によりファイル操作が認められていないと判断された場合、メッセージ表示部３５は、ＯＳ２１の表示制御部２３を介して表示装置３に「アクセスが許可されていません」等のファイル操作を拒否するメッセージを表示する（Ｓ５１）。ステップＳ４３で、処理内容判別部３４が、指示内容がファイルの操作ではないと判断した場合には、送信部３８によりＯＳ２１の処理部２４に処理が引き渡される（Ｓ５２）。処理部２４は、この指示に対応する処理を行う。

【００４６】また、システムをシャットダウンする際に

は、ＯＳ２１の入力部２２が発生する割り込み要求に対応する処理のアドレスを通常のアドレスに書き換えてから終了する。このような構成によれば、例えば、デスクトップ上で任意のプログラムの起動を指示した場合には、この指示が入力フック部３２でフックされ、判別部３７でアクセスを許可するか否かがユーザマスタファイル３９に従って判別され、許可の場合のみ、対応する暗号化・復号化プログラムが起動され、そのファイルをアクセスすることができる。

【００４７】以上説明したように、この第２の実施の形態によれば、ファイル制御プログラム３１が、入力指示を自動的に取り込んで、指示されたファイルをアクセスする権限を有するか否かをコード化指紋データに基づいて判別し、権限を有する場合にはそのファイルのアクセスを許可する。従って、ユーザに負担をかけることなくコンピュータの機密保持を実行することができる。

【００４８】また、ファイル制御プログラム３１をインストールするだけでファイル操作を制御することができ、既存のＯＳ、アプリケーションプログラム等に修正を加える必要がなく、そのまま使用することができる。

【００４９】なお、以上の説明では、起動時にファイル制御プログラム３１が、入力部２２の割り込み要求に対応する処理のアドレスを書き換えたが、ファイル制御プログラム３１のインストール時に、割り込み要求に対応する処理のアドレスを書き換え、アンインストール時に元のアドレスに書き換えてもよい。

【００５０】暗号化アルゴリズム及びそれを実現するプログラムは、データを暗号化すると共に圧縮するものが望ましく、前記復号化アルゴリズム及びそれを実現するプログラムは、暗号化されたデータを復号化すると共に伸張するものが望ましい。このような構成によれば、外部記憶装置４の記憶容量を有効に利用することができる。

【００５１】ＯＳ２１は、ＤＯＳに限定されず、いわゆる、ウインドウシステム、ｕｎｉｘ等、任意のものを使用することができる。これらのＯＳを使用する場合には、各ＯＳのプロパティに応じて、適宜ファイルへのアクセス或いは割り込みの要求、リンクの発生等の所定のイベントを検出し、指紋データの入力を促すと共に操作者がファイルをアクセスする権限を有するか否かを判別すればよい。

【００５２】なお、指紋読取装置１とコンピュータ本体とはネットワーク等で接続されてもよい。

【００５３】以上の実施の形態では、個人認証のために、コード化指紋データを使用したが、指紋データの種類は任意である。例えば、指紋の画像データをフーリエ変換し、その位相情報を抽出し、これを指紋データとして使用することも可能である。この場合は、例えば、予め登録しておいた位相情報と指紋読取装置で読み取った画像から抽出した位相情報の相関度等を比較し、相関度が一定レベル以上の場合に、２つの指紋が一致すると判断する。

【００５４】以上の実施の形態では、個人認証のために、指紋を使用したが、網膜の血管パターン、音声パターン、顔の画像等を認証情報として使用することも可能である。

【００５５】なお、この発明のコンピュータは、専用のシステムによらず、通常の指紋読取装置等と通常のコンピュータシステムを用いて実現可能である。例えば、指紋読取装置を接続したコンピュータに上述の動作を実行するためのプログラムを格納した媒体（フロッピーディスク、ＣＤ－ＲＯＭ等）から該プログラムをインストールすることにより、上述の処理を実行するコンピュータシステムを構成することができる。

【００５６】また、コンピュータにプログラムを供給するための媒体は、通信媒体（通信回線、通信ネットワーク、通信システムのように、一時的且つ流動的にプログラムを保持する媒体）でも良い。例えば、通信ネットワークの掲示板（ＢＢＳ）に該プログラムを掲示し、これをネットワークを介して配信してもよい。そして、このプログラムを起動し、ＯＳの制御下に、他のアプリケーションプログラムと同様に実行することにより、上述の処理を実行することができる。

【００５７】

【発明の効果】以上説明したように、この発明によれば、ユーザの身体情報に基づいて、ユーザにほとんど負担をかけることなく、機密を保持することができる。

【図面の簡単な説明】

【図１】本発明の第１の実施の形態によるコンピュータシステムの物理的構成を示すブロック図である。

【図２】外部記憶装置の構成を示す概念図である。

【図３】図１の制御部において実行される起動時の制御処理を示すフローチャートである。

【図４】暗号化・復号化プログラムよるデータ処理の様子を示す図である。

【図５】本発明の第２の実施の形態によるコンピュータシステムの物理的構成を示すブロック図である。

【図６】ユーザマスタファイルの例を示した図である。

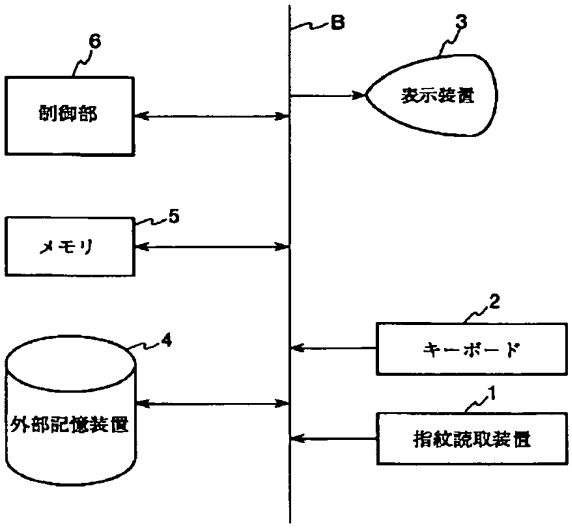
【図７】第２の実施の形態のコンピュータシステムの起動時の処理を示すフローチャートである。

【図８】第２の実施の形態のコンピュータシステムの入力操作時の処理を示すフローチャートである。

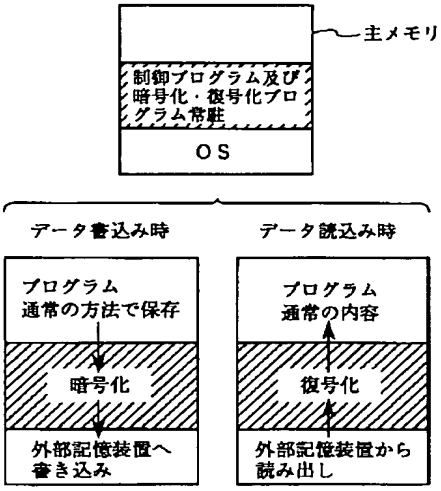
【符号の説明】

１　指紋読取装置
２　キーボード
３　表示装置
４　外部記憶装置
５　メモリ
６　制御部
１１　制御プログラム

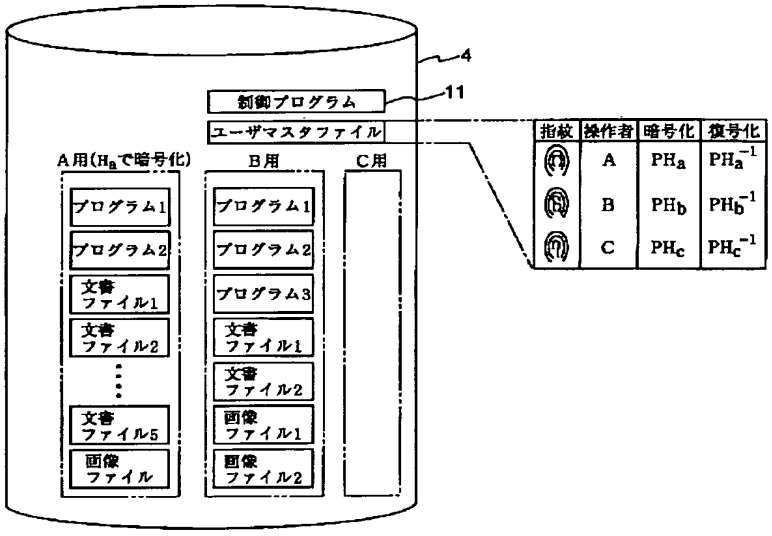
【図１】


B
3
6
制御部
表示装置
メモリ
5
2
4
キーボード
外部記憶装置
1
指紋読取装置

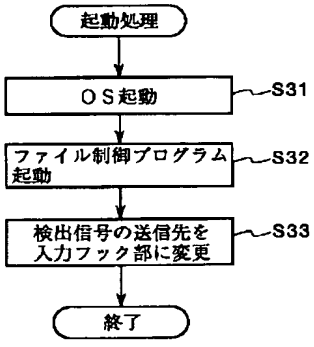
【図４】


主メモリ
制御プログラム及び暗号化・復号化プログラム常駐
ＯＳ
データ書込み時
データ読込み時
プログラム
通常の方法で保存
暗号化
外部記憶装置へ書き込み
プログラム
通常の内容
復号化
外部記憶装置から読み出し

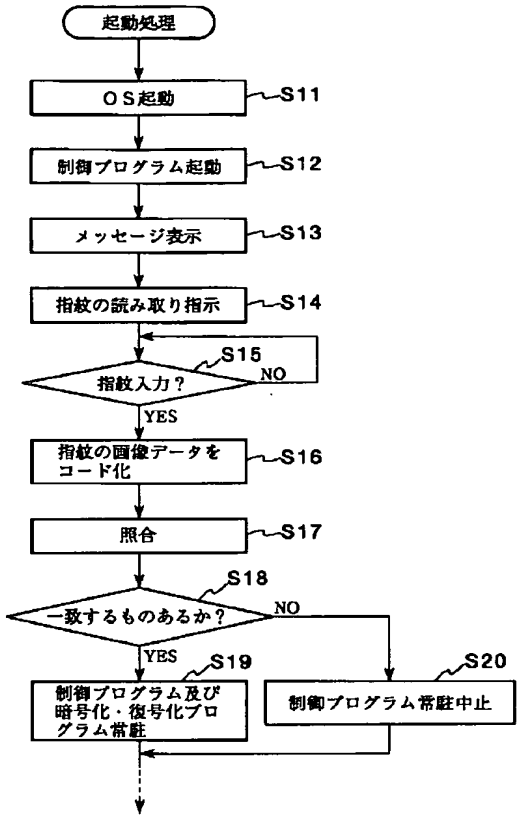
【図２】


4
制御プログラム
11
ユーザマスタファイル
指紋
操作者
暗号化
復号化
A
PHa
PHa-1
B
PHb
PHb-1
C
PHc
PHc-1
A用(Haで暗号化)
B用
C用
プログラム1
プログラム2
文書ファイル1
文書ファイル2
文書ファイル5
画像ファイル
プログラム1
プログラム2
プログラム3
文書ファイル1
文書ファイル2
画像ファイル1
画像ファイル2

【図７】


起動処理
ＯＳ起動
S31
ファイル制御プログラム起動
S32
検出信号の送信先を入力フック部に変更
S33
終了

【図３】

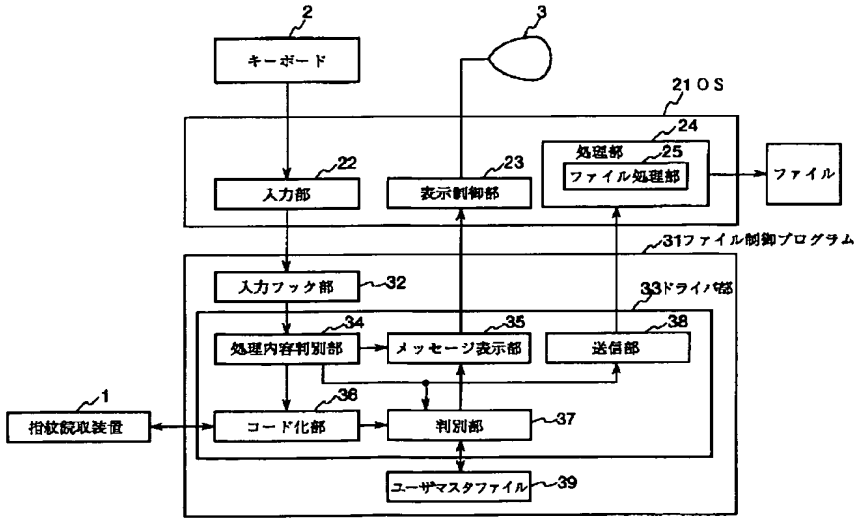


【図６】

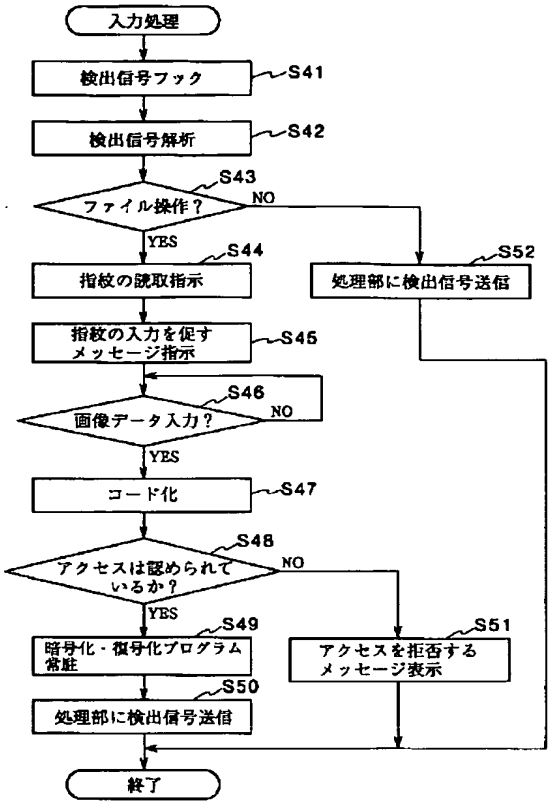
	ファイル１	ファイル２	ファイル３	……	ユーザマスタファイル
A	○	○	×	……	×
B	×	○	○	……	×
…	……	……	……	……	……
Z	○	○	○	……	○

Ｚ：システム管理者

【図５】



【図８】


入力処理
検出信号フック
S41
検出信号解析
S42
S43
ファイル操作？
NO
YES
S44
指紋の読取指示
S52
処理部に検出信号送信
指紋の入力を促す
メッセージ指示
S45
S46
画像データ入力？
NO
YES
コード化
S47
S48
アクセスは認められて
いるか？
NO
YES
S49
暗号化・復号化プログラム
常駐
S51
アクセスを拒否する
メッセージ表示
S50
処理部に検出信号送信
終了

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1]A file storage means which memorizes two or more files enciphered using two or more encryption algorithms, A characteristic storing means which matches and memorizes an operator's body information and a decryption algorithm, A decryption algorithm specifying means which searches said characteristic storing means and specifies a decryption algorithm based on an operator's body information inputted from the exterior, A processing means to decode a file memorized by said file storage means with a decryption algorithm specified by said decryption algorithm specifying means, and to access it, A computer system making accessible only a file which can be decoded with a decryption algorithm specified by a preparation and body information.
[Claim 2]A computer system comprising:
A file storage means which memorizes two or more files enciphered using two or more encryption algorithms.
An access permit condition memory measure which matches and memorizes body information of an operator permitted access of a file memorized by said file storage means and this file.
A detection means to detect a demand of access to a file memorized by said file storage means.
A means to require an input of an operator's body information when said detection means detects said demand,
An access permit discriminating means which distinguishes whether access to a file memorized by said file storage means based on physical information inputted from the exterior is accepted with reference to said access permit condition memory measure, An accessing means which makes said file accessible by loading a program for performing an algorithm which decodes this file when access was permitted and said access permit discriminating means distinguishes, and executing this program.

[Claim 3]The computer system according to claim 1 or 2 which said encryption algorithm is an algorithm which data is enciphered and is compressed, and is characterized by what is consisted of an algorithm which said decryption algorithm decrypts enciphered data, and is elongated.
[Claim 4]The computer system according to claim 1, 2, or 3 characterized by what a means to display a message which stimulates an input of body information by body information reading means which reads said operator's body information, and said body information reading means is included for.
[Claim 5]Said body information comprises fingerprint data, data of retina patterns, data of a voice pattern, or data of a face picture, and said body information reading means, The computer system according to claim 4 characterized by what comprises face a fingerprint reader, a retina-patterns reader, a voice pattern reader, or an image reader.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]Especially this invention relates to the computer system which distinguishes whether it has the authority to perform each processing from body information, such as a fingerprint, about the security art of a computer.
[0002]
[Description of the Prior Art]A user (operator) name and a password are beforehand registered into a computer for the security of a computer, When the user name and password which made enter a user name and a password at the time of logon, etc., and were entered are not registered into a computer system, the method of not accepting logon is known.
[0003]
[Problem(s) to be Solved by the Invention]However, a burden is placed on a user in security with a user name, a password, etc., such as setting up a password so that others cannot presume easily, or changing a password periodically. When user ID etc. were set up by the system administrator, the burden of memorizing and making a note of user ID was placed. Whenever there was a demand from a computer system, a user name, a password, user ID, etc. had to be inputted from the keyboard etc., and operation was complicated.
[0004]By the method of checking by user ID, whether execution is permitted by every place in a session. since there is the necessity for making a note of the user ID and the password which were given, or memorizing etc., a user may do a leaving chair during a session and the others may take a seat, security takes all possible measures -- having been hard .
[0005]This invention was made in view of the above-mentioned actual condition, and an object of an invention is to provide the computer system which does not apply the burden of security to a user.
[0006]
[Means for Solving the Problem]In order to attain the above-mentioned purpose, a computer system concerning the 1st invention, A file storage means which memorizes two or more files enciphered using two or more encryption algorithms, A characteristic storing means which matches and memorizes an operator's body information and a decryption algorithm, A decryption algorithm specifying means which searches said characteristic storing means and specifies a decryption algorithm based on an operator's body information inputted from the exterior, A processing means to decode a file memorized by said file storage means with a decryption algorithm specified by said decryption algorithm specifying means, and to access it, Only a file which can be decoded with a decryption algorithm specified by a preparation and body information was made accessible.
[0007]In order to attain the above-mentioned purpose, a computer system concerning the 2nd invention is provided with the following.
A file storage means which memorizes two or more files enciphered using two or more encryption algorithms.
An access permit condition memory measure which matches and memorizes body information of an operator permitted access of a file memorized by said file storage means and this file.
A detection means to detect a demand of access to a file memorized by said file storage means, A means to require an input of an operator's body information when said detection means detects said demand, An access permit discriminating means which distinguishes whether access to a file memorized by said file storage means based on physical information inputted from the exterior is accepted with reference to said access permit condition memory measure, An accessing means which makes said file accessible by loading a program for performing an algorithm which decodes this file when access was permitted and said access permit discriminating means distinguishes, and executing this program.

[0008]According to these composition, a decryption algorithm is specified based on an operator's body information. Therefore, each operator can access only a file which can be decoded using this decryption algorithm, and cannot access other files. Therefore, only those who have just authority can access each file. It is not necessary to enter a user name, a password, etc. one by one, and operativity is also high.
[0009]Said encryption algorithm is an algorithm which data is enciphered and is compressed, and, as for said decryption algorithm, what is consisted of an algorithm which enciphered data is decrypted and is elongated is desirable. If it has such composition, a file storage means of limited capacity can be used effectively.
[0010]A means to display a message which stimulates an input of body information by body information reading means which reads said operator's body information, and said body information reading means may be formed.
[0011]Said body information consists of fingerprint data, data of retina patterns, data of a voice pattern, data of a face picture, etc. In this case, said body information reading means comprises a fingerprint reader, a retina-patterns reader, a voice pattern reader, a face image reader, etc.
[0012]
[Embodiment of the Invention]Hereafter, this embodiment of the invention is described with reference to drawings.
(A 1st embodiment) With reference to drawing 1 - drawing 4, the computer system concerning a 1st embodiment of this invention is explained.
[0013]As shown in drawing 1, this computer system comprises the bus B which connects these with the fingerprint reader 1, the keyboard 2, the display 3, the external storage 4, the memory 5, and the control section 6.
[0014]The fingerprint reader 1 reads the picture of human being's fingerprint, and supplies the image data to the computer body 1 via an RS232C interface etc.
[0015]The keyboard 2 is an input device for inputting the data of a character, a sign, a number, etc. The display 3 comprises CRT, a liquid crystal display, etc., and displays the message to the data inputted from the keyboard 2, and an operator, etc.
[0016]The external storage 4 comprises a hard disk drive etc., and where the file (a program, a document file, a graphics file, etc. are included) which the control section 6 processes is enciphered, it is memorized. For example, in using this computer system by three persons, A, B, and C. As shown in drawing 2, the file which A accesses is enciphered by the encryption algorithm Ha, the file which B accesses is enciphered by encryption algorithm Hb, and the file which C accesses is enciphered by the encryption algorithm Hc. The external storage 4 memorizes the control program 11 and a user master file. A user master file matches and memorizes the fingerprint data of A, B, and C, enciphered program PHa-PHc, and decoded program PHa^{-1} - PHc^{-1}. The control program 11 controls encryption and a decoded program. The control program 11 is set up start following starting of OS (operating system).
[0017]The memory 5 comprises RAM (Randam Access Memory) etc., and functions as main memory, a work area, etc. of the control section 6. The control section 6 comprises MPU (Micro Processing Unit) etc., executes the program stored in main memory, and directs writing or reading of fingerprint reading, image display, and data to the fingerprint reader 1, the display 3, and the external storage 4, respectively. Processing of the image data of a fingerprint in which the control section 6 was read by the fingerprint reader 1, Processings, such as processing of Hitoshi Monju's data inputted from the keyboard 2, processing of the picture data displayed on the display 3, reading processing of the data from the external storage 4, and writing of the data to the external storage 4, are performed.
[0018]Next, operation of the computer system of this embodiment is explained with reference to the flow chart of drawing 3. If this computer system is started, first, OS will be started (S11), then the control program 11 will be started (S12).
[0019]Next, the control program 11 displays the message of a purport which should input a fingerprint on the display 3 (S13). Reading of a fingerprint is directed to the fingerprint reader 1 (S14). An operator inputs a fingerprint from the fingerprint reader 1 according to this display (S15). The fingerprint reader 1 stores the read image data (image data of a fingerprint) in the memory 5 via an interface. The control program 11 codes the image data of the fingerprint stored in the memory 5, and generates coding fingerprint data (S16). Next, coding fingerprint data and the fingerprint data of a user master file are compared (S17), and it is distinguished whether there is any match (S18).
[0020]When there is a match, it judges that it is accepted that that operator uses this computer system, and as shown in drawing 4, the control program 11, and the encryption and the decoded program corresponding to main memory (memory 5) are made resident (S19). The program data etc. which are enciphered using the decoded

program are decrypted at the time of data reading ****, and henceforth it reads, and a program is executed at the time of data writing ****, enciphering using an enciphered program and writing in program data etc.
[0021]When it is judged that the image data of the fingerprint identified in the fingerprint reader 1 is in agreement with neither of the fingerprint data registered into the user master file on the other hand (S18), The control program 11 judges that it is not accepted that that operator uses this computer system, and stops permanent residence of the control program 11 to main memory (S20). Henceforth, it shifts to the usual operation.
[0022]According to such composition, the encryption and the decoded program corresponding to [utilization time / of those who are permitted use of the computer] an operator in the control program 11 reside in main memory permanently. Therefore, as shown in drawing 2, the various data stored in the external storage 4 can be decoded by a decoded program, can be read as a usual program or data, and can be processed. Under control of the control program 11, an enciphered program can be used, it can encipher, and the data created and processed can be stored in the external storage 4.
[0023]And only the encryption and the decoded program corresponding to the operator specified with coding fingerprint data reside in main memory permanently. Therefore, each operator cannot access the file enciphered by the encryption algorithm for other operators. Therefore, access to each file can be limited to those who have just authority. On the other hand, when an operator is a non-registrant, the control program 11 does not reside in main memory permanently. Therefore, the program and various data which are stored in the external storage 4 cannot be restored. Therefore, it becomes difficult to use this system itself itself.
[0024]For example, when the operator A uses this computer system. Coincidence of the coding fingerprint data which the fingerprint was inputted at Step S15, and the image data of this fingerprint was coded at Step S16, and was generated from the image data of the fingerprint of A at Step S18, and the fingerprint data of A of a user master file will distinguish A. The enciphered program PHa and its decoded program PHa^{-1} for A reside in main memory permanently with the control program 11 (S19).
[0025]Therefore, the operator A accesses, decrypting the programs 1 and 2, the document files 1-3, a graphics file, etc. which are enciphered using the enciphered program PHa by decoded program PHa^{-1}, The document and picture which were created and processed can be enciphered and it can store in the external storage 4.
[0026]Here, even if A tends to access the file in which B has the right to access, for example, since the file of B is enciphered by the enciphered program PHb, this cannot be decrypted by decoded program PHa^{-1} which resides in main memory permanently. Therefore, A cannot access the file of B. Therefore, although the external storage 4 is shared, a file can be used for the others in the secret state.
[0027](A 2nd embodiment) In a 1st embodiment, although fingerprint data was used for the personal authentication at the time of login, it is also possible to attest an operator for example, whenever access of a file is required. A 2nd embodiment that performs such processing is described below.
[0028]The physical configuration of the computer system of this embodiment is the same as the composition fundamentally shown in drawing 1. On the other hand, logically, the computer system of this embodiment comprises OS(operating system) 21 and the file control program 31, as shown in drawing 5.
[0029]OS(operating system) 21 is provided with the input part 22 which detects the alter operation of the keyboard 2, the treating part 24 which performs processing according to the input directions detected by the input part 22, and the display control part 23 which controls the display 3. The treating part 24 contains the file processing part 25 for accessing a file.
[0030]On the other hand, the file control program 31 detects that the event occurred, and when the event is a thing about a file operation, it is a program for or or controlling [to which the file operation is permitted] whether it refuses.
[0031]Drawing 5 is an example when OS21 presupposes that it is DOS (disc operating system), and the file control program 31 comprises the input hooking portion 32, the driver part 33, and the user master file 39.
[0032]When an interrupt request is published, the input hooking portion 32 does not make the processing which should be performed when the file control program 31 does not exist (when an event occurs) perform, but makes it process to the driver part 33 in advance of this processing (it hooks).
[0033]The user master file 39 consists of every user of files, i.e., the list which can be operated for every fingerprint data, as shown in drawing 6. This user master file 39 very thing is set up so that only the administrator of this computer system can access. The driver part 33 comprises the contents discrimination section 34 of processing, the message indicator part 35, the encoding part 36, the discrimination section 37, and the transmission section 38.
[0034]The contents discrimination section 34 of processing analyzes the input incorporated by the input hooking

portion 32, when distinguishing and pointing to whether the contents are pointing to operation of a file, directs reading of a fingerprint to the encoding part 36, and it provides the discrimination section 37 with input. When the hooked input is not pointing to operation of a file, a detecting signal is sent to the transmission section 38.
[0035]The message indicator part 35 displays the screen to which the input of fingerprint information is urged on the display 3 via the display control part 23 of OS21, when the contents discrimination section 34 of processing distinguishes saying "The input is pointing to operation of a file." When the discrimination section 37 judges "the operator is not permitted the demanded file operation", the screen in which it is shown that access was refused is displayed on the display 3 via the display control part 23.
[0036]The encoding part 36 points to reading of a fingerprint to the fingerprint reader 1 according to the directions from the contents discrimination section 34 of processing, and captures the image of a fingerprint from the fingerprint reader 1, codes this, and generates coding fingerprint data.
[0037]The discrimination section 37 distinguishes whether based on the coding fingerprint data generated by the encoding part 36, those who have the coding fingerprint data have the authority to access an applicable file, with reference to the user master file 39. And when it is judged that it has authority, the signal with which access is permitted to the transmission section 38 is transmitted. When it did not have authority and distinguishes, the message of a purport which does not permit access to the message indicator part 35 is displayed.
[0038]Operation of the computer system of a 2nd embodiment is explained with reference to the flow chart of drawing 7 and drawing 8. First, an injection of the power supply of a computer will start OS21 (S31). Next, the file control program 31 starts (S32). If the input hooking portion 32 of the file control program 31 starts, it will rewrite the address of the processing corresponding to the interrupt request which the input part 22 of OS21 generates from the treating part 24 to the address of the driver part 33. A paraphrase will rewrite transmission destinations, such as a detecting signal etc. of the key operation which the input part 22 generates, to the address of the input hooking portion 32 (S33).
[0039]For example, in the case of MS-DOS (registered trademark) provided with OS21 from Microsoft Corp. Let the address of the processing corresponding to interruption INT21 of the system call about an input among the interruption table created on the memory 5 which functions as main memory be an address of the driver part 33. Above, the setting-operation at the time of starting is ended.
[0040]In this state, if there is a certain input from the keyboard 2, the input part 22 of OS21 will distinguish this alter operation, and will emit an interrupt request if needed (generating of IO event). Although processing corresponding to this interrupt request is usually performed by the treating part 24, it is rewritten by the address of the driver part 33 at the time of starting of the file control program 31. Therefore, processing shifts to the driver part 33 and is hooked (drawing 8, S41).
[0041]The contents discrimination section 34 of processing analyzes the detecting signal inputted from OS21 (S42), and distinguishes whether the entry content is pointing to operations (an executable file is started [opening a file,]) of a file (S43). When the entry content is pointing to operation of a file, reading of a fingerprint is directed to the fingerprint reader 1 via the encoding part 36 (S44). The display of the message to which the input of a fingerprint is urged is directed in the message indicator part 35 (S45). The message indicator part 35 displays the message which urges the input of a fingerprint to the display 3 via the display control part 23 of OS21 according to directions of the contents discrimination section 34 of processing.
[0042]If the input of the image data of the fingerprint from the fingerprint reader 1 is stood by (S46) and image data is inputted, the encoding part 36 changes this image data into coding fingerprint data, and provides the discrimination section 37 with it (S47). The discrimination section 37 distinguishes whether operation of a file in which those who have the coding fingerprint data supplied from the encoding part were directed by alter operation is accepted with reference to the user master file 39 (S48).
[0043]If the discrimination section 37 judges that access is accepted, it will make resident an enciphered program and a decoded program required in order to access the file at main memory (S49). Then, the discrimination section 37 supplies a detecting signal to the transmission section 38. The transmission section 38 hands over processing to the treating part 24 of OS21 (S50).
[0044]Henceforth, the treating part 24 decrypts and reads the file directed by the decoded program, enciphers by an enciphered program and writes in the data processed and generated. If access of the file is completed, the file control program 31 will delete the compression program and decoded program on main memory.
[0045]On the other hand, when it is judged at Step S48 that the file operation is not accepted by the discrimination section 37, the message indicator part 35 displays the message which refuses the file operation of "access is not permitted" to the display 3 via the display control part 23 of OS21 (S51). When the contents discrimination section 34 of processing judges that an instruction content is not operation of a file at Step S43, processing is handed over by the transmission section 38 at the treating part 24 of OS21 (S52). The treating

part 24 performs processing corresponding to these directions.
[0046]When shut [a system], it ends, after rewriting the address of the processing corresponding to the interrupt request which the input part 22 of OS21 generates to the usual address. When it points to starting of arbitrary programs on a desktop, for example according to such composition, These directions are hooked by the input hooking portion 32, it is distinguished according to the user master file 39 whether access is permitted by the discrimination section 37, only in permission, corresponding encryption and decoded program are started, and that file can be accessed.
[0047]As explained above, according to this 2nd embodiment, the file control program 31 incorporates input directions automatically, Based on coding fingerprint data, it distinguishes whether it has the authority to access the directed file, and in having authority, it permits access of the file. Therefore, security protection of a computer can be performed, without applying a burden to a user.
[0048]A file operation can be controlled only by installing the file control program 31, and it is not necessary to add correction to the existing OS, an application program, etc., and can be used as it is.
[0049]In the above explanation, at the time of starting, although the file control program 31 rewrote the address of the processing corresponding to the interrupt request of the input part 22, At the time of installation of the file control program 31, the address of the processing corresponding to an interrupt request may be rewritten, and it may rewrite to the original address at the time of uninstallation.
[0050]As for the program which realizes an encryption algorithm and it, what data is enciphered and is compressed is desirable, and, as for the program which realizes said decryption algorithm and it, what the enciphered data is decrypted and is elongated is desirable. According to such composition, the storage capacity of the external storage 4 can be used effectively.
[0051]OS21 is not limited to DOS but can use arbitrary things, such as what is called a window system and unix. What is necessary is to detect predetermined events, such as access to a file or a demand of interruption, and generating of a link, suitably, and to urge the input of fingerprint data according to the property of each OS, and just to distinguish whether an operator has the authority to access a file, in using these OS's.
[0052]The fingerprint reader 1 and a computer body may be connected in a network etc.
[0053]In an above embodiment, although coding fingerprint data was used for personal authentication, the kind of fingerprint data is arbitrary. For example, it is also possible to carry out the Fourier transform of the image data of a fingerprint, to extract the topology, and to use this as fingerprint data. In this case, for example, the correlation degree etc. of the topology registered beforehand and the topology extracted from the picture read with the fingerprint reader are measured, and when a correlation degree is more than a constant level, it is judged that two fingerprints are in agreement.
[0054]In an above embodiment, although the fingerprint was used for personal authentication, it is also possible to use the picture of the vascular pattern of the retina, a voice pattern, and a face, etc. as certification information.
[0055]The computer of this invention cannot be based on a system for exclusive use, but can be realized using the usual fingerprint reader etc. and the usual computer system. For example, the computer system which performs above-mentioned processing can be constituted by installing this program from the media (a floppy disk, CD-ROM, etc.) which stored the program for performing above-mentioned operation in the computer which connected the fingerprint reader.
[0056]Communication media (medium which holds a program temporarily and fluidly like a communication line, a communication network, and a communications system) may be sufficient as the medium for supplying a program to a computer. For example, this program may be put up for the bulletin board (BBS) of a communication network, and this may be distributed via a network. And above-mentioned processing can be performed by starting this program and performing like other application programs under control of OS.
[0057]
[Effect of the Invention]As explained above, according to this invention, secrecy can be held, without almost applying a burden to a user based on a user's body information.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1]It is a block diagram showing the physical configuration of the computer system by a 1st embodiment of this invention.
[Drawing 2]It is a key map showing the composition of an external storage.
[Drawing 3]It is a flow chart which shows the control management at the time of starting performed in the control section of drawing 1.
[Drawing 4]It is a figure showing the situation of encryption and decoded program **** data processing.
[Drawing 5]It is a block diagram showing the physical configuration of the computer system by a 2nd embodiment of this invention.
[Drawing 6]It is a figure showing the example of a user master file.
[Drawing 7]It is a flow chart which shows the processing at the time of the startup of the computer system of a 2nd embodiment.
[Drawing 8]It is a flow chart which shows the processing at the time of the alter operation of the computer system of a 2nd embodiment.
[Description of Notations]
1 Fingerprint reader
2 Keyboard
3 Display
4 External storage
5 Memory
6 Control section
11 Control program

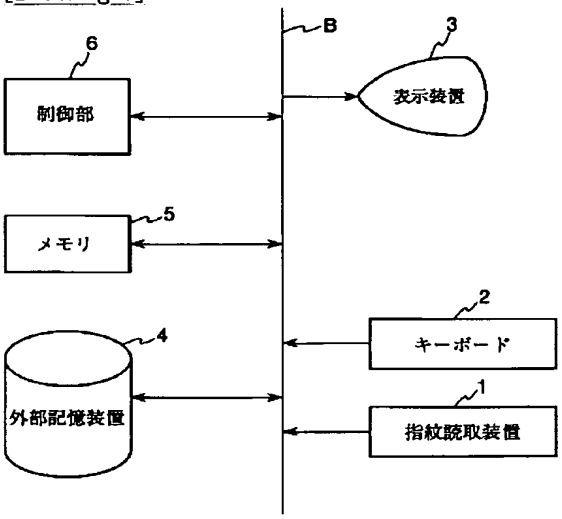
[Translation done.]

* NOTICES *

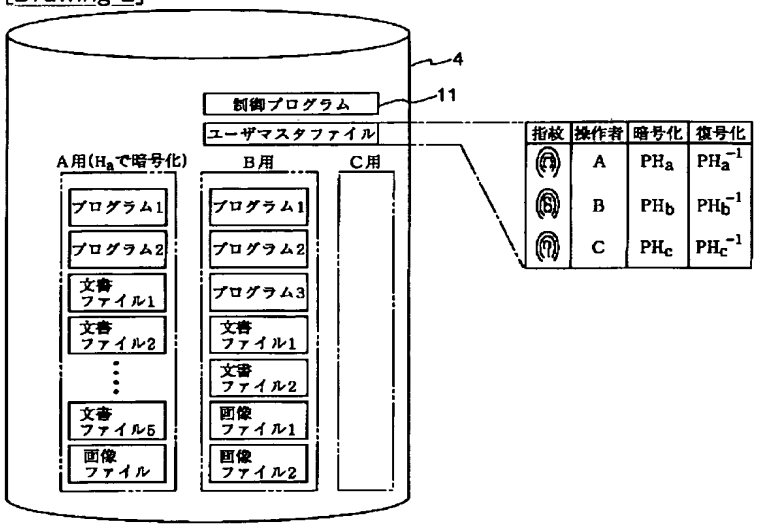
1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DRAWINGS

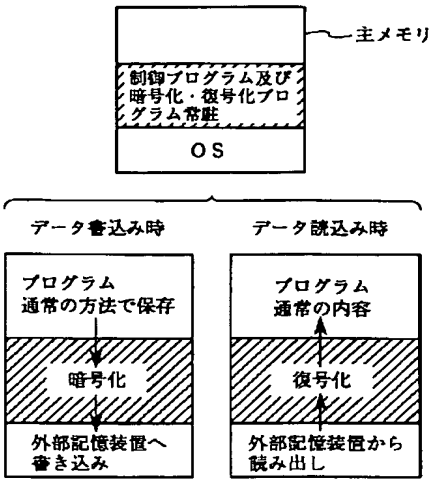
[Drawing 1]



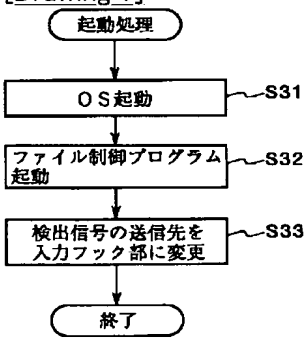
[Drawing 2]



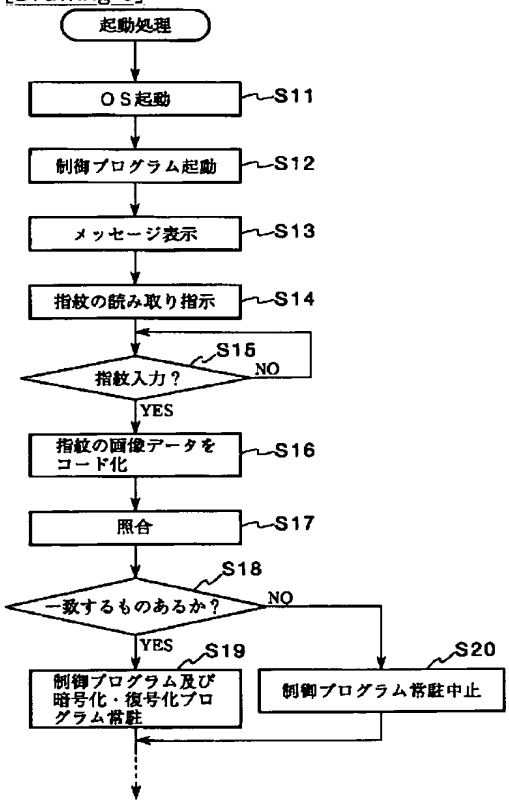
[Drawing 4]



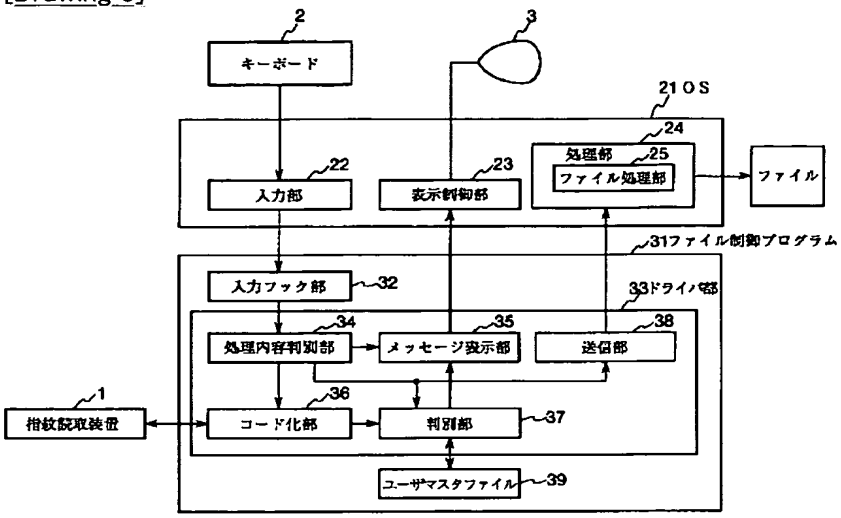
[Drawing 7]



[Drawing 3]



[Drawing 5]

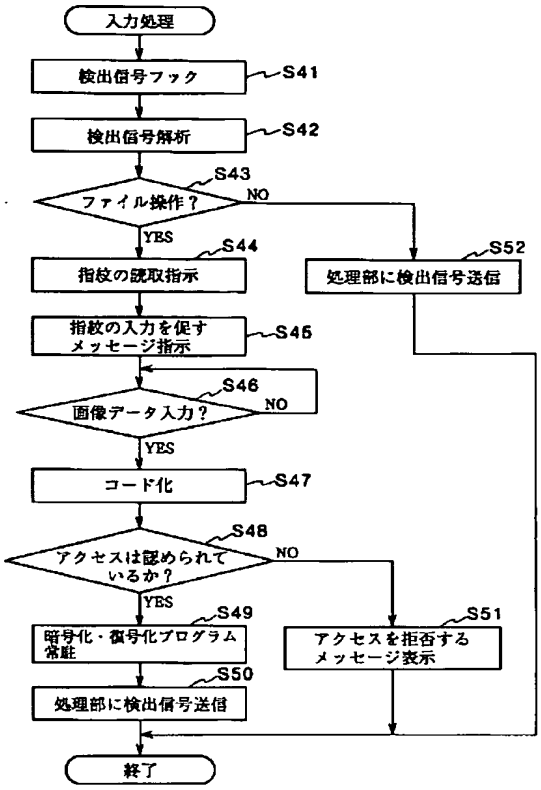


[Drawing 6]

	ファイル1	ファイル2	ファイル3	……	ユーザマスタファイル
A	○	○	×	……	×
B	×	○	○	……	×
…	……	……	……	……	……
Z	○	○	○	……	○

Z：システム管理者

[Drawing 8]



[Translation done.]